Express Mail Label:EL894234471US
Date of Deposit: June 28, 2001

ELECTRONIC WATERMARKING METHOD AND SYSTEM

FIELD OF THE INVENTION

The present invention relates to an electronic watermarking technique for digital data, and in particular to a practical and robust electronic watermarking technique.

BACKGROUND

Conventionally, electronic watermarking techniques fall into a category wherein a theoretical electronic watermarking method is applied unchanged for a variety of products, and no truly practical technique has been provided that can prevent the analyzation of an embedding algorithm. As an example, an electronic watermarking technique for digital data, an embedding and detection method used for a frequency domain, is disclosed in USP 5,687,236. According to this conventional electronic watermarking technique, embedded additive information is detected so that it can be synchronized with information (embedding start information) indicating the start of embedding. With this method, however, in addition to the additive information that originally is embedded, a synchronization signal is provided that must be used when detecting the embedded additive information. This signal must, therefore, be detected first, and accordingly, additional time is required for this purpose. Further,

when a third party, with larcenous intent, detects a synchronization signal, that party can easily analyze and extract all the embedded information. Therefore, it is generally acknowledged that a need exists for a practical and robust electronic watermarking technique.

SUMMARY OF THE INVENTION

To resolve the problems inherent to conventional electronic watermarking techniques, it is one object of the present invention to provide a practical and robust electronic watermarking method and system.

It is another object of the present invention to provide an electronic watermarking method and system for which, when they are employed for the detection of embedded additive information, a synchronization signal is not required.

It is an additional object of the present invention to provide an electronic watermarking method and system for reducing the time required for detecting embedded additive information.

It is a further object of the present invention to provide an electronic watermarking method and system for protecting an embedding algorithm and preventing it from being easily analyzed.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects, features, and advantages of the present invention will become apparent upon further consideration of the following detailed description of the invention when read in conjunction with the following drawing figures:

Fig. 1 is an example of a flowchart for a practical and robust electronic watermark embedding method according to the invention.

Fig. 2 is an example of a flowchart for a practical and robust electronic watermark detection method according to the invention.

Fig. 3 is an example of a graph for explaining a time axis, a frequency axis and bit embedding.

Fig. 4 is a diagram for explaining frame overlapping.

Fig. 5 is a diagram for explaining an amplitude change.

Fig. 6 is a diagram for explaining windowing and frame overlapping.

Fig. 7 is a diagram for explaining an example wherein there is no frame shift.

Fig. 8 is a diagram for explaining a one frame shift.

Fig. 9 is a diagram for explaining cycle synchronization.

Fig. 10 is a diagram showing an example wherein a wide frequency band is allocated while half of the additive information is regarded as more important.

Fig. 11 is a diagram for explaining diagonal embedding.

Fig. 12 is a diagram for explaining discrimination and equalization of reliability.

Fig. 13 is a diagram for explaining diagonal embedding that can increase the processing speed.

Fig. 14 is a diagram for explaining the pre-process and the post-process for the embedding process.

Fig. 15 is a diagram for explaining a method for performing re-sampling and calculating an embedding signal.

Fig. 16 is an example of a diagram for explaining another method for performing re-sampling and calculating an embedding signal.

Fig. 17 is a diagram for explaining an embedding start unit.

Fig. 18 is a diagram for explaining a virtual embedding start position.

Fig. 19 is a diagram showing a bit information embedding position that is changed as time elapses.

Fig. 20 is a diagram showing an example of the insertion of a non-information embedding position.

Fig. 21 is a diagram showing an example wherein information is embedded for which the bit is inverted at cycle 2T.

Fig. 22 is a diagram showing an example use of information other than bit information.

DETAILED DESCRIPTION OF THE INVENTION:

The present invention provides methods, systems and apparatus to achieve these and other objects. Thus, according to a first aspect of the invention, an electronic watermarking system, for embedding additive information in digital data, for which one frame is defined as including N samples extracted from digital data and a current frame is defined as a frame that is overlapped by M samples ($0<M\leqq N/2$) of a preceding frame, comprises: a frequency domain transformation unit, for multiplying a frame extracted from digital data by a window function, and for using the results to perform a Fourier transform and thus obtain a frequency component for the digital data; a frequency domain embedding unit, for employing bit information for additive information, and a frequency band for the frequency component to

change the amplitude of the frequency component in the digital data obtained by the frequency domain transformation unit; a time domain transformation unit, for performing an inverse Fourier transform to return, to a time domain signal, the frequency component whose amplitude has been changed by the frequency domain embedding unit; and an additive information embedding frame generator, for multiplying, by a window function, the time domain signal obtained by the time domain transformation unit, and for superimposing overlapped frames to generate a frame wherein the additive information is embedded.

Advantageously, to change the amplitude of the frequency component of the digital data, the frequency domain embedding unit employs bit information for additive information and the values of a mask, determined in advance in accordance with a frequency band, with which the frequency component is to be increased or decreased. advantageously, the values of the mask corresponding to all the frequencies included in one frequency band are equalized.

Advantageously, as the frequency increases, the width of the frequency band is extended.

According to a second aspect of the invention, an electronic watermark detection system, for detecting additive information embedded in digital data, comprises: a frequency domain transformation unit, for multiplying a

frame extracted from digital data by a window function, and for performing a Fourier transform to obtain a frequency component from the digital data; an amplitude storing unit, for obtaining amplitudes for the frequency components acquired by the frequency domain transformation unit, and for storing a number of the amplitudes that equals a predetermined frame count; a cycle synchronization unit, for employing an amplitude value stored by the amplitude storing unit to designate a bit detection start frame; and a bit detector, for detecting bit information from embedded additive information beginning at the bit detection start frame obtained by the cycle synchronization unit.

Advantageously, the frequency domain transformation unit uses the shorter length of the frame than the length when the additive information is embedded.

Advantageously, in order to designate the bit detection start frame by referring to the amplitude values, the cycle synchronization unit employs calculation results obtained by using the values of a mask that defines, in advance, a frequency component increase or decrease.

According to a third aspect of the invention, an electronic watermarking method, for embedding additive information in digital data, whereby one frame is defined as including N samples extracted from digital data, and a current frame is defined as a frame that is overlapped by M samples ($0<M\leqq N/2$) of a preceding frame, comprises the

steps of: extracting one frame as a current frame from digital data; multiplying the current frame by a window function; performing a Fourier transform for the resultant current frame to obtain a frequency component for the current frame; changing an amplitude of the frequency component in accordance with bit information for additive information; performing an inverse Fourier transform for the resultant frequency component; multiplying, by the window function, the frequency component obtained using the inverse Fourier transform; and adding an (N-M)-th sample, from the end of a preceding frame processed in the same manner, to an M-th sample, from the head of the current frame, and generating one new frame including N samples.

Advantageously, at the step of changing the amplitude of the frequency component, the amplitude is changed by employing bit information for additive information and the values of a mask, determined in advance in accordance with a frequency band, with which the frequency component is to be increased or decreased.

Advantageously, the values of the mask corresponding to all the frequencies included in one frequency band are equalized.

Advantageously, as the frequency increases, the width of the frequency band is extended.

According to a fourth aspect of the invention, a method

for detecting additive information embedded in digital data comprises the steps of: extracting one frame including N samples from digital data; multiplying the frame by a predetermined window function; performing a Fourier transform for the resultant frame to obtain a frequency component of the frame; storing a value for an amplitude of the frequency component; calculating an optimal start frame for additive information detection when the stored amplitude value reaches a predetermined value; and detecting bit information for the additive information beginning at the start frame.

Advantageously, at the step of extracting one frame, uses the shorter length of the frame than the length when the additive information is embedded.

Advantageously, at the step of calculating the optimal start frame, calculation results obtained by using the values of a mask, which define, in advance, a frequency component increase or decrease, are employed in order to designate the bit detection start frame by referring to the amplitude value.

According to a fifth aspect of the invention, an electronic watermarking method for embedding in digital data N bits ($N \geqq 1$) of additive information comprises the steps of: reading sample values, from digital data, up to an R-th sample ($R \geqq 1$); reading sample values, from the digital data, following an (R+1)-th sample; changing the sample values following the (R+1)-th sample in accordance

with bit information for additive information; and adding together the values up to the R-th sample in the digital data and the values following the (R+1)-th sample, changed in accordance with the bit information for the additive information.

According to a sixth aspect of the invention, an electronic watermarking method for embedding in digital data N bits (N≧1) of additive information comprises the steps of: reading a sample value from digital data; starting to change the sample value in accordance with bit information for additive information, excluding a head bit of the additive information; and using the changed sample value to generate new digital data.

According to a seventh aspect of the invention, an electronic watermarking method for embedding in digital data N bits (N≧1) of additive information comprises the steps of: reading a sample value from digital data; changing the sample value in accordance with bit information for additive information; adding noise at random to the changed sample value; and using the changed sample value to generate new digital data.

According to an eighth aspect of the invention, an electronic watermarking method for embedding in digital data N bits (N≧1) of additive information comprises the steps of: reading a sample value from digital data; changing the sample value in accordance with bit information for additive information, and setting at

random a case wherein a change is not required; and using either the changed sample value or the unchanged sample value to generate new digital data.

According to a ninth aspect of the invention, an electronic watermarking method for embedding in digital data N bits ($N \geqq 1$) of additive information comprises the steps of: changing digital data by superimposing, inserting, deleting or shifting a specific sample of the digital data; reading a sample value from the digital data; changing the sample value in accordance with bit information for additive information; and using the changed sample value to generate new digital data.

According to a tenth aspect of the invention, an electronic watermarking method for embedding in digital data N bits ($N \geqq 1$) of additive information comprises the steps of: expanding or compressing digital data along a time axis; reading a sample value from the digital data; changing the sample value in accordance with bit information for additive information; and using the changed sample value to generate new digital data. advantageously, the expansion/compression rate for the digital data does not exceed 1%.

According to an eleventh aspect of the invention, an electronic watermarking method for embedding in digital data N bits ($N \geqq 1$) of additive information comprises the steps of: reading a sample value from the digital data; changing the sample value in accordance with bit

information for additive information; using the changed sample value to generate new digital data; and expanding or compressing the new digital data along a time axis. advantageously, the expansion/compression rate for the new digital data does not exceed 1%.

According to a twelfth aspect of the invention, an electronic watermarking method for embedding in digital data N bits ($N \geqq 1$) of additive information comprises the steps of: re-sampling digital data at a sampling frequency r' and reading a sample value from the digital data; changing the sample value in accordance with bit information for additive information; and sampling the changed sample value at the original sampling frequency r to generate new digital data.

According to a thirteenth aspect of the invention, an electronic watermarking method for embedding in digital data N bits ($N \geqq 1$) of additive information comprises the steps of: sampling digital data at a sampling frequency r' and reading a sample value from the digital data; obtaining a change in the sample value in accordance with bit information for additive information; re-sampling the change at a sampling frequency r for the original digital data; and adding the re-sampled change to the original digital data to generate new digital data.

According to a fourteenth aspect of the invention, an electronic watermarking method for embedding in digital data N bits ($N \geqq 1$) of additive information comprises the

steps of: sampling digital data at a sampling frequency r, and reading a sample value from the digital data; changing the sample value in accordance with bit information for additive information; generating new digital data from the changed sample value; sampling the new digital data at a sampling frequency r', and reading a sample value; and generating newer digital data using the sample value.

According to a fifteenth aspect of the invention, a computer-readable recording medium is provided on which a program for embedding additive information in digital data is stored, the program defining one frame as including N samples extracted from digital data and defining a current frame as a frame that is overlapped by M samples ($0<M\leqq N/2$) of a preceding frame, and permitting a computer to execute: a frequency domain transformation function, for multiplying a frame extracted from digital data by a window function, and for using the results to perform a Fourier transform and thus obtain a frequency component for the digital data; a frequency domain embedding function, for employing bit information for additive information, and a frequency band for the frequency component to change the amplitude of the frequency component in the digital data obtained by the frequency domain transformation function; a time domain transformation function, for performing an inverse Fourier transform to return, to a time domain signal, the frequency component whose amplitude has been changed by the frequency domain embedding function; and an additive

information embedding frame generation function, for multiplying, by a window function, the time domain signal obtained by the time domain transformation function, and for superimposing overlapped frames to generate a frame wherein the additive information is embedded.

According to a sixteenth aspect of the invention, a computer-readable recording medium is provided on which a program for detecting additive information embedded in digital data is stored, the program permitting a computer to execute: a frequency domain transformation function, for multiplying a frame extracted from digital data by a window function, and for performing a Fourier transform to obtain a frequency component from the digital data; an amplitude storing function, for obtaining amplitudes for the frequency components acquired by the frequency domain transformation function, and for storing a number of the amplitudes that equals a predetermined frame count; a cycle synchronization function, for employing an amplitude value stored by the amplitude storing function to designate a bit detection start frame; and a bit detection function, for detecting bit information from embedded additive information beginning at the bit detection start frame obtained by the cycle synchronization function.

Example Embodiments

Example embodiments of the present invention will now be described while referring to Figs. 1 to 22. The

definitions of terms used for the embodiment are shown in Table 1, and the list of symbols is shown in Table 2. In the embodiments of the invention, an explanation will be given for an example method and an example system for employing digital audio data as example digital data for electronic watermarking. However, the electronic watermarking method and system can be applied in the same manner for digital moving picture data (MPEG, etc).

<First Embodiment>

An explanation will be given for a practical and robust electronic watermarking method and system according to a first embodiment for which frame synchronization for digital audio data is not required.

An embedding system comprises the following functions.

(1) Frequency domain transformation unit

* extraction of samples

Extracts N samples from digital audio data.

* multiplication of window function

Multiplies the extracted digital audio data by a window function.

* FFT

Performs a FFT to obtain a frequency component.

(2) Frequency domain embedding unit

The frequency domain embedding unit changes the amplitude of the frequency component, obtained by the frequency domain transformation unit, in accordance with bit information for additive information and the frequency band of the frequency

component. During this process, the frequency domain embedding unit applies an auditory psychological model for the frequency component, and calculates a permissible range wherein even when the amplitude is changed, such a change is not discerned by human beings. Then, within the permissible range, the frequency domain embedding unit changes the frequency component of the digital audio data.

(3) Time domain transformation unit

The time domain transformation unit performs an IFFT for the frequency component that has been changed. By using an inverse Fourier transform, the time domain transformation unit returns, to a time domain signal, the frequency component whose amplitude was changed.

(4) Additive information embedding frame generator

The additive information embedding frame generator multiplies, by a window function, a time domain signal obtained by the time domain transformation unit, and superimposes overlapping (adjacent) frames to generate a frame in which additive information is embedded.

A detection system comprises the following functions.

(1) Frequency domain transformation unit

* extraction of a sample

Extracts N samples from input digital audio data.

* multiplication of a window function

Multiplies extracted digital audio data by a window function.

* FFT

Performs a FFT to obtain a frequency component.

(2) Amplitude storing unit

Obtains an amplitude from a frequency component, and stores amplitudes in a number equivalent to a predetermined frame count.

(3) Cycle synchronization unit

The cycle synchronization unit designates a bit detection start frame based on the amplitude value stored by the amplitude storing unit. Values detected by the frequency domain detector are stored in a number equivalent to a predetermined frame count, and a search of the stored values is performed for the greatest absolute value, which subsequently is output as a frame shift. That is, a frame shift is effected in order to determine which frame should be the first for bit detection.

(4) Bit detector

The bit detector detects bit information for embedded additive information, beginning at the detection start frame designated by the cycle synchronization unit. Each bit is detected and output, based on the frame shift effected by the cycle synchronization unit.

Fig. 1 is an example of a flowchart for a practical and robust electronic watermark embedding method according to the embodiment. First, at step 110 one frame (N samples) is extracted from input digital data. At step 120 the extracted frame is multiplied by a window function, and

at step 130 a Fourier transform is performed for the resultant frame. As a result, the frequency component of the frame is obtained. Then, at step 140, the amplitude of the frequency component of the frame transformed into the frequency domain is changed in accordance with the additive information, while the phase of the frequency component is maintained. At this time, whether the amplitude should be increased or reduced is determined by using bit information for the additive information to be embedded in the frame and the sign of a mask corresponding to the frequency band of the frame. A change value determined by an auditory psychological model unit is employed as the amount the amplitude is to be changed. It should be noted that this change value is so calculated that, even when digital data is altered, no change in tone quality is discernible by human beings. At step 150, an inverse Fourier transform is performed for the frequency component in which the information has been embedded (the frequency component whose amplitude is changed) to return the frequency component to a signal in the time domain. At step 160, the obtained signal in the time domain is again multiplied by the window function. Finally, the resultant frame is superimposed on the preceding frame to generate a frame wherein additive information is embedded.

Fig. 2 is an example of a flowchart for a practical and robust electronic watermark detection method according to the embodiment. First, at step 210 one frame (N samples) is extracted from input digital data. At step 220, the

extracted frame is multiplied by a window function, and at step 230 a Fourier transform is performed for the resultant frame. As a result, the frequency component of the frame is obtained. Then, at step 240, the frequency components of the frame transformed in the frequency domain are stored in a number equivalent to a predetermined frame count. When the count of the stored frequency components equals the predetermined frame count, a search of the detected values is performed to locate the greatest absolute value, which subsequently is output as a frame shift (the head position of a unit). This calculation is performed using a specific mask, and a detected value is obtained with the assumption that the specific frame is located at the head position. Finally, at step 260, the detected value is selected, based on the obtained frame shift, and is compared with the frequency to determine the bit information for embedded additive information.

Equations/Expressions

In the following description all equations relating to the present invention are tabulated at the end of the text portion of this specification just prior to the claims. Each equation is given an expression number which is indicated at the place in the text below where the expression belongs.

Standard embedding and detection method

The processing performed by the embedding and detection method of the embodiment will now be described.

Additive information to be embedded

First, additive information to be embedded is represented as a symbol. The additive information consists of a bit sequence of 1s and 0s, in which all the 0s are replaced by -1s to prepare an array.
[Expression 1]
According to this method, each bit of the additive information is allocated to a frequency band having a specific width.
[Expression 2]
This expression indicates that the b-th bits from frequency lower(b) to frequency upper(b) are allocated to the frequency band, and that all the information C_w embedded in the frequencies in this range is defined as CB_b. The correlation between the bits and the frequency band is the same for all the frames. Fig. 3 is a graph showing that the frame axis (time axis) is perpendicular to the frequency axis, and that the same bit is always embedded in a specific frequency band (the same bit is represented by the portions sharing the same pattern).

[Mask]
The mask is a matrix of +1s and -1s, and since the embedding system and the detection system must both understand the function of the same mask, for this reason, the mask can serve as a type of secret key. For

the embedding system, the mask determines whether a frequency component should be increased or decreased, and for the detection system, the mask determines whether, in the detection formula, a frequency component should be added or subtracted.

[Expression 3]

[Extraction of samples]

N samples are extracted from digital audio data arranged in a time series, in which the n-th sample of an extracted frame f is represented by a(f, n). Taken collectively, these N samples form processing units called frames, each of which overlaps half of a succeeding frame. Fig. 4 is a diagram showing the overlapping of frames.

[Windowing]

A window function is multiplied to perform a FFT for a frame. Basically, a sine function is appropriate; however, any other function that satisfies the following expression can be employed. This guarantees that the digital audio data will be recovered unless the information is embedded when the frames are superimposed after the windowing has been performed twice.

[Expression 4]

In this expression, n denotes a natural number that is equal to or smaller than N/2. The sine window function is

[Expression 5]

The windowing processing is

[Expression 6]

In this expression 6, n denotes a natural number equal to or smaller than N.

[FFT]

An FFT is performed for aw(f,n) to obtain frequency component $F_{f,w}$.

[Power embedding]

During the embedding process, only the amplitude (power) is changed, the phase is unchanged.

Fig. 5 is a graph for explaining the change in the amplitude.

[Expression 7]

[IFFT]

An IFFT is performed for embedded frequency component $F'_{f,w}$ to obtain aw'(f,n).

[Windowing, superimposing frames and outputting them along a time axis]

The frame is multiplied by the window function, then the resultant frame is added to the succeeding frame and the obtained frame is output. In this fashion, the embedding of the frame in the digital audio data is completed.

[Expression 8]

According to this expression, the first half of a frame is added to the preceding frame, and the second half of the frame is added to the succeeding frame. Further, the left side of the expression refers to the digital audio

data after the embedding has been completed. When this data has been output, the embedding process for the frame f is terminated. Fig. 6 is a diagram for explaining the windowing and superimposition of frames.

[Cycle synchronization]
The detection process is performed in the same manner as the embedding process, up until the FFT process is performed to obtain the frequency component. Thereafter, the amplitude $F_{f,w}$ is obtained for each frequency, and is stored in the buffer. When the storing of amplitudes has proceeded until the requirements for the frame F have been satisfied, cycle synchronization and bit detection can be initiated. Since one part of the digital audio data may be cut off, frame f=1 is not always the first frame when the information is embedded. If the frame is shifted, the mask and the amplitude to be multiplied differ, so that a correct bit can not be detected. Fig. 7 is a diagram showing an example wherein no frame shifting has occurred, and Fig. 8 is a diagram showing an example wherein the shifting of one frame has occurred. Cycle synchronization is a process used to calculate S_s, while assuming frame shift s, and to obtain s, with which the maximum S_s is provided. Fig. 9 is a diagram for explaining cycle synchronization. For s, all the integers from 0 to (F-1) are attempted. The expression used to acquire S_s is the addition of the bit detection values. First, when frame shift s is assumed (i.e., C_w was -1 in the embedding process), the bit detection expression for bit 0 is represented by

[Expression 9]

And the bit detection expression for bit 1 (i.e., C_w was +1 in the embedding process) is represented by

[Expression 10]

In this expression, masks for the first subscript (f+s) in $M_{f+s,w}(c)$ are employed in mod F. The addition of these masks to obtain the correct bit is the detection expression used for cycle synchronization. However, since it is unclear whether the b-th bit is +1 or -1, greater values for the masks are selected and added together.

[Expression 11]

The value s with which the maximum Ss is provided is the answer for the frame shifting.

[Bit detection]

During bit detection, $C_{-,b(s)}$ and $C_{+,b(s)}$ are compared using the frame shift s, obtained during the cycle synchronization process, to determine a bit.

[Expression 12]

[Variation]

An explanation will now be given for an extension method and a replacement method employed in order to improve the basic performances of the embedding and detection systems.

[Threshold watermark value and threshold bit value]

By using the frame shift s provided by cycle synchronization, whether a watermark is embedded in the

digital audio data can be determined based on the following expression.

[Expression 13]

TMW denotes a threshold constant set in advance. The upper limit for in expression 13 may be reduced, so that a detection value for a bit embedded in a frequency band that is equal to or higher than a specific high frequency can be ignored. Further, whether the detection results obtained for each bit are reliable can also be determined.

[Expression 14]

T_b denotes a threshold value for the b-th bit. A constant difference for each bit can be employed as a threshold value, so that a high threshold value can be set for a bit that should be especially reliable.

[Employment of the same mask for several sequential frames for information embedding]

When a mask is employed for embedding information for several sequential frames, embedding signals in the overlapped frames strengthen each other and improve the detection efficiency. The same mask are employed for embedding information for several sequential frames.

[Pairing of every two frequencies]

When the denominators of expressions 9 and 10 are smaller than the numerators, the detection value can be

increased.

Of these methods, one involves the pairing of every two frequencies and the employment of a difference as a denominator. For the embedding, the sign of the odd frequency of the mask must be set opposite the sign of the succeeding arbitrary, even frequency. It should be noted that w denotes an arbitrary natural number equal to or smaller than W/2, and f denotes an arbitrary natural number equal to or smaller than F. For detection, the difference between two adjacent frequencies is obtained.

[Expression 15]

[Dividing a mask into two parts to increase the calculation speed]

According to the above method, frame shifts of 0 to (F-1) must be attempted during cycle synchronization, and expressions 9 and 10 must be calculated for each F attempts. Therefore, a mask is defined as the product of two masks as follows.

[Expression 16]

When the mask is used for embedding, the detection expression is represented by

[Expression 17]

This expression can be decomposed into

[Expression 18]

In this expression, $q_{b,f}$ does not depend on the frame shift s, and it can be calculated before cycle synchronization is initiated. Further, since $F_{f,q}$ need not be stored in the buffer, the required storage

capacity is reduced.

[Changing the width of a frequency band, and discriminating between the reliabilities of the individual bits]

The additive information to be embedded can be information concerning a copyright, copying and reproduction permission information, or information concerning music names and words, and the importance of the additive information differs greatly, depending on the information type. For example, generally the copying and reproduction permission information is more important than the music names, and is advantageously very robust. According to the method of the invention, the reliabilities of bits can be discriminated between by changing the width of each frequency band. The width of the frequency band is upper(b)-lower(b)+1, and if the width is increased, the robustness and the reliability of the bit are increased. Fig. 10 is a graph showing an example wherein a wide frequency band is allocated while the half including additive information is regarded as more important.

[Equalizing the reliabilities of bits]

Assume that the bits of additive information must have equal reliability. When each bit in the degradation process must have equal reliability, such as for a voice compression technique or radio broadcasting, wherein a band-pass filter is effective, the above method is not adequate. Because when the low-pass filter is

functional, only the bit embedded in a high frequency band is greatly deteriorated. Thus, all the bits are embedded evenly in all the frequency bands. For example, additive information to be embedded in frame f and frequency w is obtained using the following expression, and a bit is embedded diagonally.

[Expression 19]

The values in the parenthesis lower(b-f-1) and upper(b-f-1) in this expression are mod B. The positions represented by this expression for embedding individual bits are as shown in Fig. 11. The rectangles having the same pattern in Fig. 11 (representing positions in the frequency/frame plane) are those carrying the same bit. Since C_w is defined as $C_{f,w}$, the mask is defined as $M_{f,w}(C_{f,w})$.

[Expression 20]

For embedding,

[Expression 21]

For detection,

[Expression 22]

The values in parenthesis, lower(b+f-1) and upper(b+f-1), in this expression are mod B. In this embodiment, the method for regularly embedding bits diagonally has been explained; however, the embedding positions need not be arranged diagonally. For example, a secret key can be employed in the embedding process to determine a bit embedding position, and it can be also employed in the

detection process to obtain the position of a frequency component used for bit detection. Then, a system that inhibits bit detection by a party who does not know the secret key can be mounted on the above described portion.

[Discrimination and equalization of reliability]
In addition, differences in reliability can be discriminated between while specific robustness relative to the bandpass filter is provided for each bit. As one method, as is shown in Fig. 12, lower(b) and upper(b) are changed for each frame. This means the extension to lower(f,b) and upper(f,b). So long as the embedding and detection systems understand the differences between the lower(f,b) and upper(f,b), an arbitrary value can be employed. In Fig. 12, the same bit is embedded diagonally; however, the diagonal arrangement is not necessarily required. The array of the additive information is defined as
[Expression 23]

Further, the bit detection expression is defined as
[Expression 24]

[Discrimination and equalization of reliability and an increase in processing speed]
The method for increasing the processing speed will now be described. The following restrictions are provided for upper(f,b) and lower(f,b).
* The upper(f,b)-lower(f,b)+1 width of the frequency band is limited to several types.

* For bit embedding positions, only bits having the same width as the frequency band can be replaced.

Fig. 13 is a diagram for explaining diagonal bit embedding that can increase the processing speed. For example, in Fig. 13 the frequency bands are limited to two types, and less reliable bits are embedded diagonally in several narrow frequency bands, while reliable bits are embedded diagonally in wide frequency bands.

[Case wherein additive information is embedded using the positive and negative values of a mask]

According to the above method, different masks are employed for embedding bit 1 and for embedding bit 0. However, bits can be discriminated between and embedded by using the positive and negative values of one mask. In this case, only one mask is required.

[Expression 25]

For embedding, an increase or a reduction is determined in accordance with a bit.

[Expression 26]

For both cycle synchronization and bit determination, only one detection expression is formed, as follows.

[Expression 27]

As a result of this expression, both positive and negative values are obtained. In this case, it is assumed that the first subscript in mask $M_{f+s,w}$ is used for mod F. For cycle synchronization, the absolute values are obtained and added together so as to acquire the maximum, total value.

[Expression 28]
Bit determination is performed by using the positive and negative detection values.
[Expression 29]

[Returning an embedding signal to a time domain, and embedding]
When the embedding processing is changed as follows, an error that accompanies windowing or a FFT can be reduced.
(1) Extraction of samples
(2) Windowing
(3) FFT
(4) Generation of an embedding signal
The auditory psychological model is applied for a frequency component to calculate a permissible range wherein a human being can not discern a difference, even when the frequency component is changed. An embedding signal is prepared within the permissible range.
(5) IFFT
An IFFT is performed for the embedding signal.
(6) Windowing and superimposing frames, and returning the results along a time axis
The resultant frame is multiplied by a window function, and this frame is superimposed on an adjacent frame, so that the embedding signal can be obtained in the time domain.
(7) Addition of the frame to digital audio data
When the obtained frame is added to the original digital audio data, the digital audio data carrying the embedding signal is acquired and output.

For (4), the embedding signal is prepared using the following expression.

[Expression 30]

[Employment of the same mask]

When the masks that correspond to all the frequencies included in one frequency band are equalized, robustness relative to the frequency shift can be provided for the audio data. For example, when 5000Hz is changed to 5050Hz due to a frequency shift, and when different masks (signs) are used for 5000Hz and 5050Hz, the detection is adversely affected. However, when the same mask (sign) is employed, there is no adverse effect.

[Change in the width of a frequency band in accordance with a frequency]

Finally, when the width of a frequency band is extended as a frequency increases, robustness relative to an overall change in the frequency, due to a change in the music reproduction speed and a change in the length of a frame, can be provided. For this reason, since all the frequencies are increased by 10% when the reproduction speed is increased by 10%, 500Hz is changed to 550Hz and 5000Hz is changed to 5500Hz. Therefore, for a higher frequency the frequency shift is greater, and in order to provide for all the frequencies the robustness relative to a frequency shift, for a higher frequency a wider frequency band is necessary.

[Reducing a frame length to be detected]

When the length of a window (i.e., the length of a frame) for detection is shorter than the length of a window for embedding, the effect on the end of the frame being embedded can be reduced. For example, when a mask having the same sign is employed in the frequency band, assume that for embedding one frame consists of N samples and that for detection one frame consists of N/2 samples. As a result, the effect produced by the sign that was embedded in the k-th frequency is observed in the k/2-th frequency. And when one frame consists of N/4 samples for detection, the effect produced by the embedding in the k-th frequency is observed in the k/4-th frequency. This is because, according to the property of a Fourier transform, when the frame length for observation is reduced by half, the frequency resolution that is observed is also reduced by half. That is, in the detection process, when the sign of a mask is shifted a distance equivalent to the difference of a frame length, detection is enabled even when the frames differ. In this embodiment, overlapping of half or less of frames occurs, and signs are embedded while also being changed along a time axis. However, when in a specific frequency band, between adjacent frames along the time axis the signs of masks differ, the embedding effect is canceled out at the portion whereat the frames overlap (for example, when the signs are "++--" and the overlapping portions of the second and third frames differ). When a short frame length is employed for detection, as is described above, detection is enabled only for a portion

that is less affected by an adjacent frame.

<Second Embodiment>

An explanation will now be given for a second example embodiment of the present invention, which provides a practical and robust electronic watermark for digital audio data and which will prevent the unauthorized analyzation of an embedded additive information algorithm. In the following description, "sample" is the expression used when audio data is the target; however, the present invention can be applied for a moving picture by replacing "sample" with "frame", and for a static picture by replacing "sample" with "pixel".

[Determining a random embedding start position]

Before embedding, the first R samples of the content are skipped, and the embedding is performed beginning at the (R+1)-th sample. Here, R denotes a random variable determined before embedding is initiated.

[Determining a random embedding start bit or frame]

To embed multiple bits, a start bit can be determined at random. This is applicable only in a case wherein before detection a detector performs a process for determining the first bit. In this case, since the first bit should be found through this process, that bit need not always be embedded in the head of the content. The following method can be employed as a modification. According to a method for defining a specific number (F) of samples as one unit and for embedding one or multiple bits therein,

the process for finding the location whereat the pertinent unit begins is performed during the detection process. Once the head is found, the head of the content need not match the head of the unit. Thus, the sample of the unit used for the embedding start can be determined at random. Fig. 17 is a diagram showing an embedding start unit, and Fig. 18 is a diagram showing a virtual embedding start point.

[Adding random noise]

Not only an embedding signal, but also noise calculated at random is added to the content. If the amount of noise added is sufficiently small, tone quality can be prevented from being affected. And if only random noise added, it can be expected that the detection results will also be less affected.

[Occasionally adding merely a random signal, without performing embedding]

During the embedding process, a portion whereat only a random signal is to be added without performing embedding is prepared at a timing determined at random. Although this method slightly affects the detection results, since bits in other portions of the content can be detected, this method can be employed when no problem occurs, even when there are portions in which no bits are embedded.

[Performing a pre-process before embedding]

Before the embedding process, a random pre-process is performed to handle the content.

Fig. 14 is a diagram for explaining a pre-process and a

post-process for the embedding process.

Content 0 before being processed [pre-process] content 0' after the pre-process and before the embedding, and [embedding] content 0'' after embedding.

When this process is performed internally, a larcenous user can have no knowledge of the "content 0' after the pre-process and before the embedding". Therefore, even if the larcenous user knows the difference between the "content 0 before being processed" and the "content 0'' after the embedding", $D = 0''-0$, he or she will have no knowledge of the difference between the "content 0'' after the embedding" and the "content 0' after the pre-process and before the embedding", $D'' = 0''-0'$. The difference D' includes both the effect D, obtained by embedding, and the effect $D' = 0'- 0$, provided by the pre-process, and this prevents the embedding algorithm from being identified. An example pre-process is the overlapping, insertion or omission of a sample, the shifting of a sample, or the expansion/compression of a sample.

[Overlapping, insertion or omission of a sample]
For content, a sample is omitted, a specific sample is repeated, or a specific sample is inserted. This process, for music, is generally called "pitch-preserved time expansion/compression". So long as the omission, overlapping or insertion frequency is sufficiently low (e.g., one sample every 44100 samples per second), the

tone quality is not at all affected. For a static picture, this process corresponds to the overlapping, insertion or omission of a horizontal line or a vertical line. For a moving picture, a horizontal line or a vertical line for each static picture may be overlapped, inserted or omitted, or a static picture (a frame) may as one unit be overlapped, inserted or omitted. If the affect on the tone quality or the image quality is kept especially small, the location for the overlapping, insertion or omission of the image must be selected in accordance with the characteristic of the content (this is also generally performed in the pitch-preserved time expansion/compression process). For example, the target location for the omission, overlapping or insertion is limited to the portion wherein similar samples are continued. If the number of samples reduced by omission is adjusted so it is the same as the number of samples increased by overlapping or insertion, the length of the resultant content after the process can be the same as the length of the content before the process.

[Shifting of a sample]

The content is shifted a distance equivalent to the number of random samples. In other words, a sample is added to the head of the content, or is removed from the head. The number of samples is not always an integer. When the random sample count is a real number other than an integer, the sample values of the content are determined by interpolation. For example, when linear interpolation is employed, the sample value is changed by

using

[Expression 31]

In this expression, [r] denotes a maximum integer that does not exceed r, v(x) denotes an x-th sample value before the process, and v'(x) denotes an x-th sample value after the process.

[Expansion/compression]

A slight expansion/compression of the content can be performed for the object of this embodiment. For example, when the content is linearly expanded or compressed an amount that is equal to or smaller than 1%, the change can not be discerned by human beings. Further, a portion of the content may be expanded and another portion may be compressed, so that the length of the content is maintained. These methods provide great effects, even when the random pre-process is not employed. In other words, even if the pre-process is a decisive algorithm, obtaining the difference D'' is difficult, so long as the algorithm can not be identified.

[Performing the post-process after the embedding]

When the same process used for the above method, while performing the pre-process for the embedding, is used to perform the post-process for the content produced by the embedding, the same effects that prevent the analyzation of an embedding signal can be provided. In this case, since the embedding signal has also been processed, the robustness relative to the analyzation may be increased.

However, since the embedding signal is slightly deteriorated when this post-process is performed, it is predicted that the detection capability will be slightly reduced.

[Calculation of an embedding signal after re-sampling] This method is similar to the method used to perform the pre-process before the embedding, except that the original content is not changed. For a moving picture and a static picture, the re-sampling corresponds to a change in the number of pixels. The processing used for this method is performed as follows. Fig. 15 is a diagram for explaining the method for performing re-sampling and then calculating an embedding signal.

* A sampling frequency of the content 0 before the processing is defined as r.
* The content 0 is re-sampled, at a sampling frequency r', to obtain the content 0' after the re-sampling.
* A temporary embedding signal E' is obtained for the content 0'. The sampling frequency for the signal E' is also r'.
* The temporary embedding signal E' is re-sampled, at the sampling frequency r, to obtain an embedding signal E.
* The embedding signal E is added to the content 0 to obtain the content 0'' after the embedding.

As another method, as is shown in Fig. 16 (performing re-sampling and then calculating an embedding signal),
* A sampling frequency of the content 0 before the

processing is defined as r.
* The content 0 is re-sampled, at a sampling frequency r', to obtain the content 0' after the re-sampling.
* A temporary embedding signal E' is obtained for the content 0'. The sampling frequency for the signal E' is also r'.
* The temporary embedding signal E' is added to the content 0', to prepare the content 0'', after the embedding is performed at the sampling frequency r'.
* The content 0'' is re-sampled, at the sampling frequency r to obtain the content 0'''.

The sampling frequency used for embedding may be determined at random for the embedding process. Even when the sampling frequency is not determined at random, it is considered to be an effective means for hiding the algorithm. According to this method, when the sample count (the unit in Figs. 17 and 18) is employed as a reference to generate an embedding signal, identifying the length of the samples is difficult.

[Setting a random interval for outputting detection results]

This is not a method for substantially preventing the analyzation of a difference; however, since this method is the same as another method used to for prevent the analyzation of an algorithm, this method will be explained. According to this method, when the detection results are obtained, instead of an action such as the display of results or the halting of copying, the output

is intentionally delayed at specific, randomly determined time intervals. Therefore, the minimum time required for detection is prevented from being identified by a larcenous user.

[Time change of bit information embedding position]
When N bits ($N \geqq 1$) of information is to be embedded as an electronic watermark in image or audio content, the embedding position for each bit of the bit information embedding unit (hereafter referred to as a unit) is changed as time elapses. Thus, even when a specific position in the bit information embedding content is processed or destroyed, disabling of the detection or the alteration of only specific bit information can be avoided. Further, even when the information is the same, it is embedded in different positions, so that the embedding signals do not strengthen each other even if the average of multiple contents is obtained. This is advantageous as it makes it difficult to analyze the electronic watermarking algorithm and the key. Assuming that the n-th bit information embedding position at time t (unit number) is defined as $P(n,t)$, the n-th bit information embedding position at time t+1 can be represented by $P(n,t+1)=F(P(n,t))$. $F(P)$ denotes a transform operator for changing a bit information embedding position, and P and $F(P)$ have a specific cycle T.
[Expression 32]

Fig. 19 is a diagram showing an example of P and F(P)

wherein four bits of information is embedded in one unit. Each block indicated by a solid line in Fig. 19 represents a unit, and the small numbered blocks in the units represent the positions used for embedding bit information.

In this example,
P(n,t)=t+n mode 4 (T=4, n=0, 1, 2, 3).
When F(P) is complicated and the length is extended, it is more difficult to assume the bit information embedding position and to disable the detection of specific bit information and to alter specific bit information.

Further, as time elapses, not only the bit information embedding position, but also the interpretation of the embedded information can be changed. In addition, according to this method, when the original target content for electronic watermarking has a correlation along the time axis, the correlation can be canceled because the bit information embedding position is changed as time elapses. As a result, a false positive error ratio, at which the presence of embedded information is determined, even though no information is actually present, can be reduced.

[Detection]
Since the bit information embedding position in the unit is changed as time elapses, the embedded information should be detected in the following manner for each cycle of the change in the bit information embedding position.

[Expression 33]

In this expression, D(P(n,t)) denotes an operator for electronic watermark detection at the information embedding position in each unit, and Dn denotes a detection value. When the information embedding bit count N≧2, and when the content in which information is embedded is processed, the position of a detection value that represents the first information embedding bit can not be identified. Thus, the position of the first information embedding bit must be detected. This method will now be described.

When the information embedding bit count N≧2, the detection value Dn that represents the position of the first information embedding bit is detected using one of the following methods.

[Insertion of position where no information is to be embedded]
At the same cycle T as the bit information embedding position change cycle T, a position whereat no information is to be embedded is inserted as a mark for detecting the first embedded bit. For example, in P and F(P) in Fig. 19, a portion shown in Fig. 20, whereat no information is to be embedded, is inserted. Assume that the shaded portions in Fig. 20 are those whereat no information is to be embedded in the frame. When the detection value of the information embedding position satisfies |Dn|>Th, the n-th detection value that

satisfies $\min(|Dn|) < Th$ can be obtained as a mark for locating the first embedded bit. It should be noted that Th is a specific threshold value.

[Embedding of information for which the bit is inverted at cycle 2T]
At the same cycle T as the bit information embedding position change cycle T, information for which the bit is inverted at cycle 2T is embedded. Fig. 21 is a diagram showing an example of the embedding of information for which the bit is inverted at cycle 2T. Assume that + or - in Fig. 21 represents the bit-inversion information. During the detection process, at cycle 2T each detection value is calculated based on expression 33, and the n-th detection value that satisfies expression 34 is examined.
[Expression 34]
Then, the first bit of the embedded information can be obtained. In this case, the following expression is established.
[Expression 35]

[Use of information other than bit information]
The detection value of another signal is employed to detect the first bit for embedded information. For example, when unit positioning information (sink information) is embedded for the electronic watermark detection, during the bit information embedding process the sign of the pertinent signal is inverted for each embedding position change cycle T. Or, a portion having an inverted sign is inserted each cycle T. As a result,

in the detection process, when the portion is examined whereat the sign of the positioning information is changed, the position of the first bit can be obtained. Fig. 22 is a diagram showing an example for using information other than the bit information.

[Change of interpretation of embedded information]
To repetitively embed a specific bit in content, the sign of the bit is inverted in accordance with a specific sign sequence. Since the same information is not constantly embedded, the analyzation of information is difficult. The information to be embedded at a specific time is calculated using the following expression.
[Expression 36]

In this expression, B denotes the original bit information (1 or -1; a bit is represented as 0 or -1), and B'(t) denotes a bit, which is actually embedded in the content, having a sign that is inverted as time elapses. M(t) denotes a sign sequence for inverting the embedded information, and a value +1 or -1 is provided. As is described above, when the interpretation of the embedded information is to be changed as time elapses, the detection values Dn should also be obtained by using the interpretation change method M(t) as in
[Expression 37]
However, it should be noted that when the content in which the information is being embedded is processed, the detection of the value D(P(n, T)) at each position P(n, t) must be synchronized with M(t). When the correct

synchronization is acquired, M(t) is multiplied twice during the embedding and the detection processes to provide a value of +1, so that the original bit information can be obtained. To synchronize the process, one of the following methods is employed.

[+/- inversion]

Assume M(t+1) =-M(t) is the interpretation method M(t). In order to correctly interpret the embedded bit information, first, the value D(P(n,t)) detected at each location P(n,t) is multiplied by a sequence wherein signs are inverted at adjacent times, and the detection value Dn is obtained. When correct synchronization with M(t) is acquired, the bit information can be correctly detected. When the correct synchronization is not obtained, all the signs + and - are inverted, and the resultant sign sequence is multiplied by each value D(P(n,t). Thus, the inverted bit information is detected. Therefore, information Wm for determining whether the inverted bits are detected is embedded at a position other than the bit information embedding position. When the embedded bit information is detected, the sign of the information Wm is examined, and the bit information is re-interpreted as [Expression 38] Then, the embedded bit information is obtained.

[Application of the maximum detection value]

A sequence is prepared that has, as the interpretation change method M(t), a cycle T', and has the maximum value T' only when

[Expression 39]

is established with j =m*T' (m is a natural number). During the detection process, the detection values are calculated by shifting the method M(t), and the shifting distance required to provide the maximum detection value is obtained to effect the synchronization with the interpretation change method M(t).

[Expression 40]

[Employment of information other than bit information]

The detected bit interpretation M(t) is provided as the detection value for another signal. For example, when unit positioning information (sink information, represented as S(t)) is embedded for electronic watermark detection, during the embedding of the bit information, the sign to which the pertinent signal is inverted is the same as that sign of the M(t). During the detection process, the sink information is detected, and its sign for the sink information is used for bit interpretation.

[Expression 41]

According to the present invention, a practical and robust electronic watermarking method and system are provided that do not require the embedding of a frame synchronization signal. Further, since frame synchronization is not required, the detection time can be reduced. In addition, the storage capacity normally required for a detection system to provide frame synchronization is not necessary. Thus, an electronic watermarking method and system are provided that make it

difficult for a larcenous third party to analyze an embedding algorithm.

The present invention can be realized in hardware, software, or a combination of hardware and software. The present invention can be realized in a centralized fashion in one computer system, or in a distributed fashion where different elements are spread across several interconnected computer systems. Any kind of computer system - or other apparatus adapted for carrying out the methods described herein - is suitable. A typical combination of hardware and software could be a general purpose computer system with a computer program that, when being loaded and executed, controls the computer system such that it carries out the methods described herein. The present invention can also be embedded in a computer program product, which comprises all the features enabling the implementation of the methods described herein, and which - when loaded in a computer system - is able to carry out these methods.

Computer program means or computer program in the present context mean any expression, in any language, code or notation, of a set of instructions intended to cause a system having an information processing capability to perform a particular function either directly or after conversion to another language, code or notation and/or reproduction in a different material form.

It is noted that the foregoing has outlined some of the more pertinent objects and embodiments of the present invention. This invention may be used for many applications. Thus, although the description is made for particular arrangements and methods, the intent and concept of the invention is suitable and applicable to other arrangements and applications. For example, in many applications and/or embodiments of the present invention the term 'including' as used herein in this description and in some of the claims often is also given the meaning of the words 'consisting of'. It will be clear to those skilled in the art that other modifications to the disclosed embodiments can be effected without departing from the spirit and scope of the invention. The described embodiments ought to be construed to be merely illustrative of some of the more prominent features and applications of the invention. Other beneficial results can be realized by applying the disclosed invention in a different manner or modifying the invention in ways known to those familiar with the art.

The following is a tabulation of the equations relating to the present invention. The expression number of each equation corresponds with the expression number given at the place in the text above where the expression belongs.

[Expression 1]

$$CB = [CB_1, CB_2, \dots, CB_b, \dots, CB_B]$$
$$= [+1, +1, \dots, -1, \dots, +1]$$

[Expression 2]

$$C_w = CB_b \qquad (lower(b) \leq w \leq upper(b))$$

[Expression 3]

$$M = \begin{bmatrix} M_{1,1}(C_1) & \cdots & M_{1,W}(C_W) \\ \vdots & M_{f,w}(C_w) & \vdots \\ M_{F,1}(C_F) & \cdots & M_{F,W}(C_W) \end{bmatrix}$$

[Expression 4]

$$w(n)^2 + w(n+N/2)^2 = 1$$

[Expression 5]

$$w(n) = \sin\left(\pi \frac{n}{N}\right)$$

[Expression 6]

$$aw(f,n) = w(n) \times a(f,n)$$

[Expression 7]

$$F'_{f,w} = F_{f,w} \times \left\{ 1 + M_{f,w}(C_w) \times \frac{P_{f,w}}{F_{f,w}} \right\}$$

$$I'_{f,w} = I_{f,w} \times \left\{ 1 + M_{f,w}(C_w) \times \frac{P_{f,w}}{F_{f,w}} \right\}$$

$$R'_{f,w} = R_{f,w} \times \left\{ 1 + M_{f,w}(C_w) \times \frac{P_{f,w}}{F_{f,w}} \right\}$$

[Expression 8]

$$a'(f,n) = \begin{cases} w(n) \times aw'(f,n) + w(n+N/2) \times aw'(f-1,n+N/2) & (0<n\leq N/2) \\ w(n) \times aw'(f,n) + w(n-N/2) \times aw'(f+1,n-N/2) & (N/2<n\leq N) \end{cases}$$

[Expression 9]

$$c_{-,b}(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[\frac{\sum_{w=lower(b)}^{upper(b)} M_{f+s,w}(-1) \times F_{f,w}}{\sqrt{\sum_{w=lower(b)}^{upper(b)} (F_{f,w})^2}} \right]$$

[Expression 10]

$$c_{+,b}(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[\frac{\sum_{w=lower(b)}^{upper(b)} M_{f+s,w}(+1) \times F_{f,w}}{\sqrt{\sum_{w=lower(b)}^{upper(b)} (F_{f,w})^2}} \right]$$

[Expression 11]

$$S_s = \sum_{b=1}^{B} \max\{c_{-,b}(s), c_{+,b}(s)\}$$

[Expression 12]

$$\text{b-th bit} = \begin{cases} 1 & (c_{+,b}(s) > c_{-,b}(s)) \\ 0 & (c_{+,b}(s) < c_{-,b}(s)) \end{cases}$$

[Expression 13]

$$\text{Watermark} \begin{cases} \text{Yes} & \left(\frac{1}{\sqrt{B}} \sum_{b=1}^{B} \max\{c_{-,b}(s), c_{+,b}(s)\} > TWM \right) \\ \text{No} & \mathit{otherwise} \end{cases}$$

[Expression 14]

$$\text{b-th bit} = \begin{cases} 1 & (c_{+,b}(s) - c_{-,b}(s) > T_b) \\ 0 & (c_{-,b}(s) - c_{+,b}(s) > T_b) \\ \text{No reliable bit information} & \mathit{otherwise} \end{cases}$$

[Expression 15]

$$c_b = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[\frac{\sum_{w=\frac{lower(b)}{2}}^{\frac{upper(b)}{2}} M_{f,2w-1}(F_{f,2w-1} - F_{f,2w})}{\sqrt{\sum_{w=\frac{lower(b)}{2}}^{\frac{upper(b)}{2}} (F_{f,2w-1} - F_{f,2w})^2}} \right]$$

[Expression 16]

$$M_{f,w} = MF_f \times MW_w$$

[Expression 17]

$$c_b(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[\frac{\sum_{w=lower(b)}^{upper(b)} M_{f+s,w} F_{f,w}}{\sqrt{\sum_{w=lower(b)}^{upper(b)} (F_{f,w})^2}} \right]$$

$$= \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[MF_{f+s} \frac{\sum_{w=lower(b)}^{upper(b)} MW_w F_{f,w}}{\sqrt{\sum_{w=lower(b)}^{upper(b)} (F_{f,w})^2}} \right]$$

[Expression 18]

$$c_b(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} [MF_{f+s} \times q_{b,f}]$$

$$q_{b,f} = \frac{\sum_{w=lower(b)}^{upper(b)} MW_w F_{f,w}}{\sqrt{\sum_{w=lower(b)}^{upper(b)} (F_{f,w})^2}}$$

[Expression 19]

$$C_{f,w} = CB_b \qquad (lower(b\text{-}f+1) \le w \le (upper(b\text{-}f+1))$$

[Expression 20]

$$M = \begin{bmatrix} M_{1,1}(C_{1,1}) & \cdots & M_{1,W}(C_{1,W}) \\ \vdots & M_{f,w}(C_{f,w}) & \vdots \\ M_{F,1}(C_{F,1}) & \cdots & M_{F,W}(C_{F,W}) \end{bmatrix}$$

[Expression 21]

$$F'_{f,w} = F_{f,w} \times \left\{ 1+M_{f,w}(C_{f,w}) \times \frac{P_{f,w}}{F_{f,w}} \right\}$$

[Expression 22]

$$c_{+,b} = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[\frac{\sum_{w=lower(b+f-1)}^{upper(b+f-1)} M_{f,w}(+1) \times F_{f,w}}{\sqrt{\sum_{w=lower(b+f-1)}^{upper(b+f-1)} (F_{f,w})^2}} \right]$$

$$c_{-,b} = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[\frac{\sum_{w=lower(b+f-1)}^{upper(b+f-1)} M_{f,w}(-1) \times F_{f,w}}{\sqrt{\sum_{w=lower(b+f-1)}^{upper(b+f-1)} (F_{f,w})^2}} \right]$$

[Expression 23]

$$C_{f,w} = CB_b \qquad (lower(f,b) \leq w \leq (upper(f,b))$$

[Expression 24]

$$c_b(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[\frac{\sum_{w=lower(f,b)}^{upper(f,b)} M_{f+s,w} \times F_{f,w}}{\sqrt{\sum_{w=lower(f,b)}^{upper(f,b)} (F_{f,w})^2}} \right]$$

[Expression 25]

$$M = \begin{bmatrix} M_{1,1} & \cdots & M_{1,W} \\ \vdots & M_{f,w} & \vdots \\ M_{F,1} & \cdots & M_{F,W} \end{bmatrix}$$

[Expression 26]

$$F'_{f,w} = F_{f,w} \times \left(1 + M_{f,w} \times \frac{P_{f,w}}{F_{f,w}}\right)$$

$$I'_{f,w} = I_{f,w} \times \left(1 + M_{f,w} \times \frac{P_{f,w}}{F_{f,w}}\right)$$

$$R'_{f,w} = R_{f,w} \times \left(1 + M_{f,w} \times \frac{P_{f,w}}{F_{f,w}}\right)$$

[Expression 27]

$$c_b(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[\frac{\sum_{w=lower(b)}^{upper(b)} M_{f+s,w} F_{f,w}}{\sqrt{\sum_{w=lower(b)}^{upper(b)} (F_{f,w})^2}} \right]$$

[Expression 28]

$$S_s = \sum_{b=1}^{B} | C_b(s) |$$

[Expression 29]

$$\text{b-th bit} = \begin{cases} 1 & (c_b(s) > 0) \\ 0 & (c_b(s) < 0) \end{cases}$$

[Expression 30]

$$\Delta F_{f,w} = M_{f,w}(C_w) \times P_{f,w} \times \frac{F_{f,w}}{F_{f,w}}$$

$$\Delta I_{f,w} = M_{f,w}(C_w) \times P_{f,w} \times \frac{I_{f,w}}{F_{f,w}}$$

$$\Delta R_{f,w} = M_{f,w}(C_w) \times P_{f,w} \times \frac{R_{f,w}}{F_{f,w}}$$

[Expression 31]

$$v'(x) = ([x+\tau] + 1 - (x+\tau)) \times v([x+\tau]) + ((x+\tau) - [x+\tau]) \times v([x+\tau] + 1)$$

[Expression 32]

$$P(n,t+T) = F^{T}(P(n,t)) = P(n,t)$$

[Expression 33]

$$D_n = \sum_{i=0}^{T-1} D(F^{i}(P(n,t+i)))$$

[Expression 34]

$$D0_n \cdot D1_n < 0$$

[Expression 35]

$$D0_n = \sum_{i=0}^{T-1} D(F^{i}(P(n,t+i)))$$

$$D1_n = \sum_{i=T}^{2T-1} D(F^{i}(P(n,t+i)))$$

[Expression 36]

$$B'(t) = B \times M(t)$$

[Expression 37]

$$D_n = \sum_{i=0}^{T-1} D(F^i(P(n,t+i))) \times M(t)$$

[Expression 38]

$$D_n = D_n \quad (if\ Wm_{bitrev} > 0)$$
$$D_n = -D_n \quad (if\ Wm_{bitrev} < 0)$$

[Expression 39]

$$Conv(j) = \sum_{i=0}^{T'-1} M(t+j+i) \times M(t+i)$$

[Expression 40]

$$D_n = \max_{0 \le j \le T'} \left(\sum_{i=0}^{T-1} D(F^i(P(n,t+i))) \times M(t+j) \right)$$

[Expression 41]

$$D_n = \sum_{i=0}^{T-1} D(F^i(P(n,t+i))) \times \sin(S(t))$$